VAN HOVEN DECL.
ISO OPPOSITION TO INTUITIVE'S MOTION TO REOPEN DISCOVERY

EXHIBIT 13

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SURGICAL INSTRUMENT SERVICE COMPANY, INC. Plaintiff/Counter-Defendant	) Civil Action No.:) 3:21-cv-03496-VC
Vs.	)
INTUITIVE SURGICAL, INC., Defendant/Counterclaimant	)

HIGHLY CONFIDENTIAL ATTORNEYS' EYES ONLY

Deposition of PAUL D. MARTIN, Ph.D., was taken via videotape and Zoom on Thursday, March 16, 2023, commencing at 10:32 a.m., at 12102 Ashcroft Terrace, Monrovia, Maryland, before MICHELE D. LAMBIE, Notary Public.

Reported By:

Michele D. Lambie, CSR-RPR

APPEARANCES:

ON BEHALF OF THE PLAINTIFF/COUNTER-DEFENDANT:

McCaulley Law Group.

JOSHUA VAN HOVEN, ESQUIRE.

josh@mccaulleylawgroup.com.

3001 Bishop Drive.

Suite 300.

San Ramon, California 94583.

(925) 302-5941

ON BEHALF OF THE DEFENDANT/COUNTERCLAIMANT:

Covington & Burling LLP.

KATHRYN ELIZABETH CAHOY, ESQUIRE.

kcahoy@cov.com.

3000 El Camino Real.

5 Palo Alto Square.

Palo Alto, California 94306.

(650) 632-4700

APPEARANCES CONTINUED:

ON BEHALF OF THE DEFENDANT/COUNTERCLAIMANT:

Covington & Burling LLP.

MIRIAM ARGHAVANI, ESQUIRE.

marghavani@cov.com.

415 Mission Street.

Suite 5400.

San Francisco, California 94105.

(415) 591-7059

ALSO PRESENT: Nolan Church - Videographer

Paul Baker - Concierge

EXAMINATION INDEX

EXHIBITS INDEX

(Attached to Transcript.)

MS. CAHOY: Objection to form.

BY MR. VAN HOVEN:

Q. That's something that's possible?

A. You would need to have a system set up to allow for that.

Q. Is the -- to your knowledge, is the use counter value that's stored on a CryptoRF chip in an Xi EndoWrist, is that value stored in -- in an encrypted form?

A. My understanding is that -- you said on an EndoWrist X/Xi. My understanding is that that value along with some other values are encrypted on that -- on those devices.

Q. What type of encryption is used for that?

(Whereupon, there was a pause for document examination.)

THE WITNESS: I don't think that's entirely clear from what I have seen.

BY MR. VAN HOVEN:

Q. So, you don't know what type of encryption is used for the use counter on the Xi

EndoWrist; is that right?

A. I think that's right. The evidence that I have seen has been conflicting on that front and in one case incorrectly referenced SHA as a type of encryption.

Q. But you don't personally know what type of encryption is used for the use counter on the Xi EndoWrist, right?

A. I don't believe I know all of the specifics of the cryptography used to encrypt the use counter and other information on the CryptoRF chips.

Q. What specifics do you know of the cryptography -- cryptography used to encrypt the use counter on the Xi EndoWrists?

A. I know the information in the datasheet about various things that are supported with respect to cryptography on these chips.

Q. But you don't know what Intuitive uses within that datasheet?

A. I don't know what they ultimately

selected.

Q. If you were tasked to attempt to circumvent the encryption of the use counter on the Xi EndoWrist, how would you go about that?

MS. CAHOY: Objection to form.

THE WITNESS: Oh, that's like a really complicated question. I don't think I could -- that's an entire like work engagement. That would take a lot of analysis just to figure out how to even approach the problem.

BY MR. VAN HOVEN:

Q. But let's just assume that you have access to the Atmel CryptoRF chip that has a use counter value on it that is encrypted, okay?

A. Okay.

Q. In that, you can either physically or wirelessly communicate with the chip?

A. Okay.

Q. And that you have the datasheet that tells you the types of encryption that's implemented, --

A. Um-hum.

Q. -- right? And you -- you have that datasheet, right?

A. Yes.

Q. So, given that information based on your 15 to 20 years of information security experience, as a general approach, how would you go about trying to circumvent the encryption on the use counter within an Atmel CryptoRF chip?

A. So, I -- I just haven't done that analysis.

Q. I understand. I'm -- but you're here to testify as an expert in the area of information security and I just want to understand the general approach you would take.

MS. CAHOY: Objection to form.

THE WITNESS: Right. So, the problem is it's a specific problem for a specific chip, and I would need to do a good amount of legwork to figure out what that approach would be. I haven't done that legwork, so I don't know what my approach

would be.

BY MR. VAN HOVEN:

Q. What type of legwork is typically involved in trying to attack that sort of problem?

A. I would need to spend some time thinking about it.

Q. So, time is one piece of -- one part of that legwork?

A. I don't think time is what I would call part of any legwork. Time is just a resource that you need to have to do anything.

In the absence of any time at all, everything would stand still, right? So, it's not clear what that means.

Q. I'm not talking about us getting close to the speed of light or anything here, but I'm just trying to understand, you said that there would be legwork. And I'm just trying to, what is -- what is the kind of legwork that -- that you're envisioning to attack the problem of circumventing the encryption as we've described on the Atmel

CryptoRF chip?

A. Sure. So, the -- the truth is that's -- that's complicated, and I haven't really thought about it.

Q. But you'd have to think about it a little bit, right?

A. Yes, I would have to think about that.

Q. You'd have to look at the datasheet?

A. Certainly, looking at the datasheet would be a part of any legwork.

Q. You would have to --

A. That would be true.

Q. Excuse me. You would have to perform some sort of direct electrical or in -- indirect communication channel probing of the chip probably?

MS. CAHOY: Objection to form.

THE WITNESS: At -- at some stage in the process, you would need to connect to the chip, but I haven't really thought about when or how that would occur. So, I don't have any more insight into that.

BY MR. VAN HOVEN:

Q. Do you think that the encryption employed by the CryptoRF chip is particularly complicated compared to the sort of encryption you typically have worked with?

A. I don't have an opinion on that.

Q. You don't know one way or the other?

A. I would need to investigate it more to figure it out.

Q. And you understand or do you have an understanding that, that the use counter value at some point is transmitted from the EndoWrist to the robot?

A. Yes.

Q. Do you know if that value is transmitted in that encrypted form or if it's decrypted before it's transmitted?

A. I understand the value to be encrypted when it's transmitted.

Q. What's the basis of that understanding?

A. My understanding is from the datasheet

counting data areas of the RFID tag are one-time programmable.

That means they can be -- not be modified once written. Though, of course, they could be decremented, which is an important point.

And so it reads to me that Intuitive documents state that the data is encrypted both at rest and in motion.

BY MR. VAN HOVEN:

Q. And your opinion in that regard is based solely on those documents, right?

MS. CAHOY: Objection to form.

THE WITNESS: I can also see that the datasheet supports those configurations.

BY MR. VAN HOVEN:

Q. As far as the encryption while the -- and here I'm talking specifically about the communications between the Xi EndoWrist and the Xi robot.

As far as the encryption while the data is at motion -- in motion, what would be your

approach to try -- if you were trying to circumvent that encryption?

A. Well, that's -- again, that's sort of the same problem as trying to reverse engineer or break the chip and -- as whole, right?

If I could circumvent that communication, then I would know how -- if I knew how to do that, I would know how to break the communication protocol, so it's the same issue. I don't -- I haven't performed that analysis. I don't know.

Q. But -- but that is your -- your primary area of expertise and study over the last 20 years, right?

A. Yes, I've done many of these. They always require a very thorough set of, you know, thoughts and research and legwork before you can really come up with an approach, and I haven't done that. I haven't done that part of what my normal practice would be.

Q. Yeah. So, if you were to approach a problem like this in your normal practice, what

sort of legwork would you need to perform?

A. Right. So, I would need to look at the individual issues at play, and I would need to look at the product and how it's designed. Let me just think about it and come up with an approach, and that would kind of let me determine what legwork I need to do to then -- so, I would need to think about what I would need to know. Then I would need to think about from what I needed to know, I would know that -- learn that information and figure out from that what I would do to attack.

So, it's a multi-step process, and I haven't performed even the first step yet is the problem.

Q. You just haven't examined that for the Xi EndoWrist, right?

A. That's right. Yeah, I haven't performed an analysis of what would be required to break the device.

I reviewed Mr. Humphrey's analysis. I saw that wouldn't work, but I haven't performed an